CLAIMS

What is claimed is:

1. An apparatus for encrypting/decrypting data, said apparatus comprising:

a first plurality of encryption tables, each of the encryption tables being capable of transforming a data value into an encrypted/decrypted value, the data value corresponding to a unit of the data, the encrypted/decrypted value corresponding to a unit of encrypted/decrypted data;

a second plurality of selection tracks, each of the selection tracks including a series of values having a certain pattern;

a track mixer coupled to said second plurality of selection tracks, adapted to combine corresponding values of the selection tracks to produce a series of combined values; and

an encryption/decryption module coupled to said first plurality of encryption tables and said track mixer, adapted to transform each unit of the data into a unit of encrypted/decrypted data using an encryption table selected for that unit in accordance with a combined value in the series of combined values.

2. The apparatus in accordance with claim 1, further comprising:

a selection track generator adapted to generate the second plurality of selection tracks from a plurality of source files.

3. The apparatus in accordance with claim 1, further comprising:

a data step size selector adapted to select a data length for the unit.

4. The apparatus in accordance with claim 3 wherein the data length is one byte.

5. The apparatus in accordance with claim 3 wherein the data length is less than one byte.

6. The apparatus in accordance with claim 3 wherein the data length is more than one byte.

7. The apparatus in accordance with claim 1 wherein operations of said table selector and said encryption/decryption module are synchronized.

8. The apparatus in accordance with claim 1 wherein the data is a stream of data transmitted in real time.

9. The apparatus in accordance with claim 1 wherein the encrypted/decrypted data is a stream of data transmitted in real time.

10. The apparatus in accordance with claim 1 wherein said first plurality of encryption tables include:

a first table bank including encryption tables adapted to transform an original data value into an encrypted value; and

a second table bank including encryption tables adapted to transform the encrypted value into the original data value.

11. The apparatus in accordance with claim 1 wherein said first plurality of encryption tables include:

first encryption tables adapted to transform the data value into the encrypted/decrypted value; and

second encryption tables adapted to transform the data value into the encrypted/decrypted value, each of the second encryption tables being capable of inverse-transforming the encrypted/decrypted value that is encrypted/decrypted by a corresponding first encryption table into an original data value, each of the first encryption tables being capable of inverse-transforming the encrypted/decrypted data value that is encrypted/decrypted by a corresponding second encryption table into an original data value.

12. The apparatus in accordance with claim 11 wherein each of the first plurality of encryption tables is associated with a tables location address, and the second encryption tables have the tables location addresses a predetermined amount offset from that of the corresponding first encryption table.

13. The apparatus in accordance with claim 11 wherein said encryption/decryption module includes:

a table selector coupled to said first plurality of encryption tables and said track mixer, said table selector being adapted to associate a combined value in the series with a tables location address.

14. The apparatus in accordance with claim 13 wherein said table selector is further adapted to

select the encryption tables using the series of combined values if the data is to be encrypted; and

select the encryption tables using the series of combined values with the predetermined offset if the data is to be decrypted.

15. The apparatus in accordance with claim 13 wherein said table selector is adapted to

select the encryption tables using the series of combined values if the data is to be transmitted; and

select the encryption tables using the series of combined values with the predetermined offset if the data is received.

16. The apparatus in accordance with claim 11, further comprising:

a look-up table providing an one-to-one association between each of the first encryption tables and the corresponding second encryption table.

17. The apparatus in accordance with claim 1 wherein the encryption table is capable of transforming each of possible data values into a corresponding encrypted/decrypted value which is also one of the possible data values different from the original data value.

18. The apparatus in accordance with claim 1 wherein said selection track generator includes:

a memory storing a plurality of source files; and

a track pattern manager coupled to said memory, adapted to generate a series of values from a selected source files.

19. The apparatus in accordance with claim 18 wherein said track pattern manager is further adapted to modify each of the series of values using setting parameters.

20. The apparatus in accordance with claim 18 wherein said track pattern manager is further adapted to select a mathematical operation to be used to combine the value of each track with other tracks.

21. An apparatus in accordance with claim 1, further comprising:

an identification code unique to said apparatus; and

a first database memory containing said first plurality of encryption tables and said second plurality of selection tracks as an encryption/decryption file associated with the identification code.

22. The apparatus in accordance with claim 21 wherein said first database memory further includes, as the encryption/decryption file:

a set of setting parameters capable of modifying values of each of said selection tracks and determining a manner of combination of each selection track to other tracks.

23. The apparatus in accordance with claim 21, further comprising:

a second database memory designated to store at least one second encryption/decryption file different from the encryption/decryption file on the first database memory.

24. The apparatus in accordance with claim 23 wherein the encryption/decryption file on the first memory is adapted to encrypt the second encryption/decryption file for transmission, or to decrypt the second encryption/decryption file which is encrypted.

25. The apparatus in accordance with claim 1, wherein each of the selection tracks has a key length by which the certain pattern of the track recurs.

26. The apparatus in accordance with claim 25, wherein the key length of a selection track is different from the key length of another selection track.

27. The apparatus in accordance with claim 26, wherein none of the key length is obtained by multiplying another key length by 2^n, or by dividing another key length by 2^n, where n is an integer.

28. The apparatus in accordance with claim 25, wherein differences among the key lengths are substantially smaller than the key lengths.

29. A method for encrypting/decrypting original data into encrypted/decrypted data, said method comprising:

providing a first plurality of encryption tables, each encryption table being capable of transforming a data value into an encrypted/decrypted value, the data value corresponding to a unit of the data, the encrypted/decrypted value corresponding to a unit of encrypted/decrypted data;

providing a second plurality of selection tracks, each selection track including a series of values having a certain pattern;

combining corresponding values of the selection tracks to produce a series of combined values;

selecting an encryption table for each unit of the data in accordance with a corresponding combined value in the series of combined values; and

transforming each unit of the data into a unit of encrypted/decrypted data using the encryption table selected for that unit.

30. The method in accordance with claim 29, further comprising:

selecting the second plurality of source files from among source files stored in a database memory; and

producing a series of values from each of the selected source files.

31. The method in accordance with claim 30, further comprising:

modifying each of the series of values using setting parameters.

32. The method in accordance with claim 31, further comprising:

selecting a mathematical operation to be used to combine the value of each track with other tracks.

33. The method in accordance with claim 32, further comprising:

pre-processing at least one of

said selecting the second plurality of source files,

said producing a series of values,

said modifying,

said selecting a mathematical operation, and

said combining corresponding values; and

storing in a database memory at least one of

the series of values produced from the selected source files,

the series of values modified by the setting parameters, and

the series of combined values.

34. The method in accordance with claim 29, further comprising:

selecting a data length of the unit.

35. The method in accordance with claim 34 wherein the data length is one byte.

36. The method in accordance with claim 34 wherein the data length is less than one byte.

37. The method in accordance with claim 34 wherein the data length is more than one byte.

38. The method in accordance with claim 29, further comprising:

synchronizing said selecting and said transforming.

39. The method in accordance with claim 29 wherein the data is a stream of data transmitted in real time.

40. The method in accordance with claim 29 wherein the encrypted/decrypted data is a stream of data transmitted in real time.

41. The method in accordance with claim 29 wherein said first plurality of encryption tables include:

a first table bank including encryption tables adapted to transform an original data value into an encrypted value; and

a second table bank including encryption tables adapted to transform the encrypted value into the original data value.

42. The method in accordance with claim 29 wherein the first plurality of encryption tables includes:

first encryption tables adapted to transform the data value into the encrypted/decrypted value; and

second encryption tables adapted to transform the data value into the encrypted/decrypted value, each of the second encryption tables being capable of inverse-transforming the encrypted/decrypted value that is encrypted/decrypted by a corresponding first encryption table into an original data value, each of the first encryption tables being capable of inverse-transforming the encrypted/decrypted data value that is encrypted/decrypted by a corresponding second encryption table into an original data value.

43. The method in accordance with claim 42 wherein each of the first plurality of encryption tables is associated with a tables location address, said method further comprising:

associating the second encryption tables with the tables location addresses a predetermined amount offset from that of the corresponding first encryption table.

44. The method in accordance with claim 43 wherein said selecting an encryption table includes:

selecting the encryption tables using the series of combined values if the data is to be encrypted; and

selecting the encryption tables using the series of combined values with the predetermined offset if the data is to be decrypted.

45. The method in accordance with claim 43 wherein said selecting an encryption table includes:

selecting the encryption tables using the series of combined values if the data is to be transmitted and

selecting the encryption tables using the series of combined values with the predetermined offset if the data is received.

46. The method in accordance with claim 42, further comprising:

providing a one-to-one association between each of the first encryption tables and the corresponding second encryption table.

47. The method in accordance with claim 29 wherein the encryption table is capable of transforming each of possible data values into a corresponding encrypted/decrypted value which is also one of the possible data values different from the original data value.

48. The method in accordance with claim 29 wherein said selecting an encryption table includes:

associating a combined value in the series with a tables location address;

selecting an encryption table associated with the tables location address.

49. A method for automatically setting up an encryptor/decryptor on an apparatus, the apparatus including an identification code unique to the apparatus and a setup file associated with the identification code, the setup file being capable of encrypting/decrypting data, said method comprising:

receiving the identification code from the apparatus;

retrieving the setup file associated with the identification code from a data base memory containing setup files;

creating a session file, including

selecting a set of encryption tables from among a plurality of encryption tables;

selecting a set of selection tracks from among a plurality of selection tracks, each of the selection tracks including a series of values having a certain pattern; and

selecting a set of setting parameters from among a plurality of setting parameters;

associating the session file with the identification code;

encrypting the information of the session file using the setup file; and

transmitting the encrypted information of the session file to the apparatus.

50. The method in accordance with claim 49 wherein the information of the session file includes:

the set of encryption tables;

the set of selection tracks; and

the set of setting parameters.

51. The method in accordance with claim 49 wherein the information of the session file includes at least one of:

indication of which encryption tables are to be used;

indication of which selection tracks are to be used; and

indication of which setting parameters are to be used.

52. The method in accordance with claim 49, further comprising:

storing, in a database memory, the information of the session file with an association with the identification code.

53. The method in accordance with claim 52, further comprising:

storing, in a second database memory at a different location, at least one of the set of encryption tables, the set of selection tracks, and the set of setting parameters with association with the identification code.

54. The method in accordance with claim 52 wherein the second database memory is accessible from the apparatus via a computer network.

55. The method in accordance with claim 49 wherein said selecting a set of selection tracks includes:

selecting a source file containing data capable of producing a certain pattern; and

selecting a software module capable of generating a certain pattern.

56. The method in accordance with claim 49 wherein said selecting a set of encryption tables includes:

selecting a set of encryption tables of the setup file.

57. The method in accordance with claim 49 wherein said selecting a set of selection tracks includes:

selecting at least one selection tracks of the setup file.

58. The method in accordance with claim 49 wherein said selecting a set of setting parameters includes:

selecting a least one setting parameter of the setup file.

59. A method for authenticating an apparatus having an identification code unique to the apparatus and a setup file associated with the identification code, the setup file being capable of encrypting/decrypting data, said method comprising:

receiving the identification code from the apparatus;

retrieving a setup file associated with the identification code from a data base memory containing setup files;

generating a sequence of values and transmitting the sequence to the apparatus;

encrypting the sequence using the retrieved setup file;

calculating a first check sum from the encrypted sequence;

receiving from the apparatus a second check sum which is calculated at the apparatus from an encrypted sequence using the setup file thereof;

determining if the second check sum matches the first check sum; and

authenticating the apparatus if the second check sum matches the first check sum.

60. An apparatus for automatically setting up an encryptor/decryptor on a second apparatus, the second apparatus including an identification code unique to the second apparatus and a setup file associated with the identification code, the setup file being capable of encrypting/decrypting data, said apparatus comprising:

means for receiving the identification code from the second apparatus;

means for retrieving the setup file associated with the identification code from a data base memory containing setup files;

means for selecting a set of encryption tables from among a plurality of encryption tables;

means for selecting a set of selection tracks from among a plurality of selection tracks, each of the selection tracks including a series of values having a certain pattern produced using a source file;

means for selecting a set of setting parameters from among a plurality of setting parameters;

means for associating the set of encryption tables, the set of selection tracks, and the set of setting parameters with the identification code;

means for encrypting the set of encryption tables, the set of selection tracks, and the set of setting parameters using the setup file; and

means for transmitting the encrypted set of encryption tables, the encrypted set of selection tracks, and the encrypted set of setting parameters to the second apparatus.

61. The apparatus in accordance with claim 60, further comprising:

means for storing, in a database memory, the set of encryption tables, the set of selection tracks, and the set of setting parameters with an association with the identification code.

62. The apparatus in accordance with claim 61, further comprising:

means for storing, in a second database memory at a different location, at least one of the set of encryption tables, the set of selection tracks, and the set of setting parameters with association with the identification code.

63. The apparatus in accordance with claim 62, wherein the second database memory is accessible from the second apparatus via a computer network.

64. An apparatus for authenticating a second apparatus having an identification code unique to the second apparatus and a setup file associated with the identification code, the setup file being capable of encrypting/decrypting data, said apparatus comprising:

means for receiving the identification code from the second apparatus;

means for retrieving a setup file associated with the identification code from a data base memory containing setup files;

means for generating a sequence of values and transmitting the sequence to the second apparatus;

means for encrypting the sequence using the retrieved setup file;

means for calculating a first check sum from the encrypted sequence;

means for receiving from the second apparatus a second check sum which is calculated at the second apparatus from an encrypted sequence using the setup file thereof;

means for determining if the second check sum matches the first check sum; and

means for authenticating the second apparatus if the second check sum matches the first check sum.

65. A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform a method for encrypting/decrypting original data into encrypted/decrypted data, said method comprising:

providing a first plurality of encryption tables, each encryption table being capable of transforming a data value into an encrypted/decrypted value, the data value corresponding to a unit of the data, the encrypted/decrypted value corresponding to a unit of encrypted/decrypted data;

providing a second plurality of selection tracks, each selection track including a series of values having a certain pattern produced using a corresponding source file;

combining corresponding values of the selection tracks to produce a series of combined values;

selecting an encryption table for each unit of the data in accordance with a corresponding combined value in the series of combined values; and

transforming each unit of the data into a unit of encrypted/decrypted data using the encryption table selected for that unit.

66. A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform a method for automatically setting up an encryptor/decryptor on an apparatus, the apparatus including an identification code unique to the apparatus and a setup file associated with the identification code, the setup file being capable of encrypting/decrypting data, said method comprising:

receiving the identification code from the apparatus;

retrieving the setup file associated with the identification code from a data base memory containing setup files;

selecting a set of encryption tables from among a plurality of encryption tables;

selecting a set of selection tracks from among a plurality of selection tracks, each of the selection tracks including a series of values having a certain pattern produced using a source file;

selecting a set of setting parameters from among a plurality of setting parameters;

associating the set of encryption tables, the set of selection tracks, and the set of setting parameters with the identification code;

encrypting the set of encryption tables, the set of selection tracks, and the set of setting parameters using the setup file; and

transmitting the encrypted set of encryption tables, the encrypted set of selection tracks, and the encrypted set of setting parameters to the apparatus.

67. A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform a method for authenticating an apparatus having an identification code unique to the apparatus and a setup file associated with the identification code, the setup file being capable of encrypting/decrypting data, said method comprising:

receiving the identification code from the apparatus;

retrieving a setup file associated with the identification code from a data base memory containing setup files;

generating a sequence of values and transmitting the sequence to the apparatus;

encrypting the sequence using the retrieved setup file;

calculating a first check sum from the encrypted sequence;

receiving from the apparatus a second check sum which is calculated at the apparatus from an encrypted sequence using the setup file thereof;

determining if the second check sum matches the first check sum; and

authenticating the apparatus if the second check sum matches the first check sum.

68. A pseudo-random number generator, comprising:

a selection track generator adapted to generate a plurality of selection tracks, each selection track including a series of values having a certain pattern produced using a corresponding source file; and

a track mixer coupled to said selection track generator, adapted to combine corresponding values of the selection tracks to produce a series of combined values.

69. The pseudo-random number generator in accordance with claim 68 wherein said selection track generator includes:

a memory storing a plurality of source files; and

a track pattern manager coupled to said memory, adapted to generate a series of values from a selected source file.

70. The pseudo-random number generator in accordance with claim 69 wherein said track pattern manager is further adapted to modify each of the series of values using setting parameters.

71. The pseudo-random number generator in accordance with claim 68 wherein said track pattern manager is further adapted to select a mathematical operation to be used to combine the value of each track with other tracks.

72. The pseudo-random number generator in accordance with claim 68 wherein each of the selection tracks has a key length by which the certain pattern of the track recurs.

73. The pseudo-random number generator in accordance with claim 73 wherein none of the key length of the selection track is equal to another key length.

74. The pseudo-random number generator in accordance with claim 72, wherein none of the key length is obtained by multiplying another key length by 2^n, or by dividing another key length by 2^n, where n is an integer.

75. The pseudo-random number generator in accordance with claim 73, wherein differences among the key lengths are substantially smaller than the key lengths.